Amendments to the claims:

Please amend the claims as indicated below. Added text is underlined and deleted text is either struck through or enclosed in double brackets. Applicant avers that no new matter is being added.

1. (Currently amended) A method for accelerating delivery of requested secure webpages comprising:

~~a) receiving a request for a secure webpage, the request made using a link in a first received webpage which has been rewritten from an original format at a client proxy such~~rewriting, with a client proxy, original format links in first webpages identifying secure webpages so that any request for [[the]] a secure webpage made by referencing [[the]] a rewritten link [[is]] will be recognized by an intermediating device intermediating between a client and a server capable of responding to the request for the secure webpage;

receiving a request, for the secure webpage, made using a rewritten link in a received webpage;

[[b)]] returning the ~~request~~ rewritten link to its original format to thereby accelerate delivery of the requested secure webpage;

[[c)]] requesting the secure webpage from the server; and

[[d)]] receiving the requested secure webpage from the server.

2. (Currently amended) The method of claim 1 further comprising the client proxy scanning the ~~first~~ received webpage for any link to a secure webpage.

3. (Currently amended) The method of claim 1 further comprising establishing a secure connection between the intermediating device and the server responding to the request for the secure webpage.

4. (Currently amended) The method of claim 1 wherein an https ~~request~~ link in the ~~first~~ received webpage is rewritten to be an http ~~request~~link.

5. (Currently amended) The method of claim 1 wherein an https ~~request~~ link in the ~~first~~ received webpage is rewritten to include a reference to a subdomain recognized by the intermediating device as indicating a request for a secure webpage.

6. (Currently amended) The method of claim 5 further comprising establishing a secure connection between the client and the intermediating device when the request for the secure webpage is received at the intermediating device.

7. (Original) The method of claim 1 further comprising returning any received webpage to the client proxy.

8. (Original) The method of claim 1 further comprising returning any received webpage to the client.

9. (Original) The method of claim 1 further comprising decrypting the secure webpage.

10. (Original) The method of claim 1 further comprising compressing the secure webpage.

11. (Currently amended) The method of claim 10 wherein compressing the secure webpage includes:

[[a)]] compressing data with encoder software ~~acting as an encoder, the software~~ running on ~~a first device in~~ an encoder communicating via a network ~~communication~~ with other devices, the compressed data to be transmitted to a decoder~~second device~~ in the network, running decoder software ~~acting as a decoder~~, the compressing consisting of representing runs of data with at least one identifier;

[[b)]] storing the at least one identifier and corresponding data represented by the at least one identifier in a database associated with the encoder; and

[[c)]] transmitting from the encoder to the decoder, data corresponding to the at least one identifier when the data is specifically requested by the decoder or when the encoder has no record of the at least one identifier being sent to the decoder.

12. (Currently amended) The method of claim 11 ~~further including representing~~wherein runs of ~~identifiers~~ data are represented with a single identifier.

13. (Currently amended) The method of claim 11 further including transmitting from the encoder to the decoder only data required to complete a response to the request ~~where~~ when the data has not been cached at a ~~second~~ database associated with the decoder.

14. (Currently amended) A method for accelerating delivery of requested secure webpages comprising:

[[a)]] scanning a webpage to determine whether it contains any links to ~~at least one~~ secure webpage<u>s</u>;

[[b)]] rewriting any link to ~~at least one~~ <u>a</u> secure webpage such that a request for the secure webpage made by referencing the rewritten link [[is]] <u>will be</u> recognized by a<u>n intermediating</u> device intermediating between a client and a server capable of responding to the request for the secure webpage;

[[c)]] delivering the scanned webpage to the ~~requesting~~ client;

[[d)]] receiving a ~~rewritten~~ request for a secure webpage at the <u>intermediating</u> device, ~~said~~ <u>the</u> request based on the rewritten link;

[[e)]] returning the <u>rewritten link in the</u> request to its original format <u>to thereby accelerate delivery of the requested secure webpage</u>;

[[f)]] requesting the secure webpage from the server; and

[[g)]] receiving the requested webpage from the server.

15. (Original) The method of claim 14 wherein an https request is rewritten to be an http request.

16. (Currently amended) The method of claim 14 wherein an https request is rewritten to include a reference to a subdomain recognized by the ~~proxy~~ <u>intermediating device</u> as indicating a request for a secure webpage.

17. (Currently amended) The method of claim 14 further comprising establishing a secure connection between the <u>intermediating</u> device and the server responding to the request for the secure webpage.

18. (Currently amended) The method of claim [[16]] 14 further comprising establishing a secure connection between the client and the intermediating device.

19. (Original) The method of claim 14 further comprising decrypting the received webpage.

20. (Currently amended) The method of claim 14 further comprising compressing the requested ~~received~~ webpage.

21. (Original) The method of claim 14 further comprising returning the received webpage to the client proxy.

22. (Original) The method of claim 14 further comprising returning the received webpage to the client.

23. (Currently amended) The method of claim 20 wherein compressing the secure webpage includes:

[[a)]] compressing data with encoder software ~~acting as an encoder~~, ~~the software~~ running on ~~a first device in~~ an encoder communicating via a network ~~communication~~ with other devices, the compressed data to be transmitted to a ~~second device~~decoder in the network, the decoder running decoder software ~~acting as a decoder~~, the compressing consisting of representing runs of data with at least one identifier;

[[b)]] storing the at least one identifier and corresponding data represented by the at least one identifier in a database associated with the encoder; and

[[c)]] transmitting from the encoder to the decoder, data corresponding to the at least one identifier when the data is specifically requested by the decoder or when the encoder has no record of the at least one identifier being sent to the decoder.

24. (Currently amended) The method of claim 23 ~~further including representing~~wherein runs of ~~identifiers~~ data are represented with a single identifier.

25. (Currently amended) The method of claim 23 further including transmitting from the encoder to the decoder only data required to complete a response to the request ~~where~~ when the data has not been cached at a ~~second~~ database associated with the decoder.

26. (Currently amended) A system for accelerating delivery of requested secure webpages in a network comprising:

[[a)]] a client having first software means for requesting and receiving secure and nonsecure webpages;

[[b)]] a plurality of servers having second software means for responding to a client's request for secure and nonsecure webpages;

[[c)]] a client proxy having means for rewriting links, to any secure webpage in a webpage requested ~~and received~~ by the client, ~~the links rewritten~~ from ~~their~~ an original format of the links such that the client's request for a secure webpage based on a rewritten link [[is]] will be recognized as a request for a secure webpage by an intermediating device intermediating between the client and the plurality of servers; and

[[d) a]] the intermediating device intermediating between the client and the plurality of servers, ~~the device~~ having third software means for recognizing the rewritten link in a request for a secure webpage, returning the ~~request~~ rewritten link to ~~its~~ the original format, and using the ~~original~~ request with the rewritten link in the original format to obtain the secure webpage from one of the plurality of servers to thereby accelerate delivery of a requested secure webpage.

27. (Currently amended) The system of claim 26 ~~further comprising~~wherein the client proxy ~~having~~ comprises means for delivering a requested webpage to the client.

28. (Currently amended) The system of claim 26 ~~further comprising~~wherein the intermediating device ~~having~~ comprises means for delivering a requested webpage to the client proxy.

29. (Currently amended) The system of claim 26 ~~further comprising~~wherein the client proxy ~~having~~ comprises means for scanning ~~the~~ any received webpage for any links to [[a]] secure webpages.

30. (Currently amended) The system of claim 26 ~~further comprising~~ wherein the intermediating device ~~having~~ comprises means for setting up a secure connection between the intermediating device and the ~~server~~ one of the plurality of servers responding to the request for the secure webpage.

31. (Currently amended) The system of claim 26 wherein the means for rewriting links to any secure webpage rewrites an https request [[is]] to be an http request.32. (Currently amended) The system of claim 31 wherein the means for rewriting links to any secure webpage rewrites ~~an~~ the https request to include a reference to a subdomain recognized by the intermediating device ~~as indicating~~to thereby indicate a request for a secure webpage.

33. (Currently amended) The system of claim 32 ~~further comprising~~wherein the client ~~having~~ comprises means for establishing a secure connection between the client and the intermediating device.

34. (Currently amended) The system of claim 26 wherein the client and the intermediating device are members of a private network.

35. (Currently amended) The system of claim 26 wherein the ~~server~~ one of the plurality of servers is a member of a public network.

36. (Currently amended) The system of claim 26 ~~further comprising~~wherein the intermediating device ~~having~~ comprises means for decrypting the webpage.

37. (Currently amended) The system of claim 26 ~~further comprising~~wherein the intermediating device ~~having~~ comprises means for compressing the webpage.

38. (Currently amended) The system of claim 37 ~~further comprising~~wherein the client proxy ~~having~~ comprises means for decompressing the webpage.

39. (new) A method to reduce processing requirements on a client requesting secure content from a remote server over the Internet, the method comprising:

identifying a link to a secure webpage received from the remote server by the client;

rewriting the link to be recognizable by an intermediating device disposed between the client and the remote server;

enabling the intermediating device to intercept the rewritten link and retrieve the secure webpage;

receiving the requested secure webpage from the server onto the intermediating device; and

sending the requested secure webpage from the intermediating device to a client proxy.

40. (new) The method of claim 39 wherein the step of identifying a link to the secure webpage is selected to be performed by the client proxy.

41. (new) The method of claim 39 wherein the step of rewriting the link changes a secure request to a non-secure request.

42. (new) The method of claim 39 wherein the step of rewriting the link redirects a secure request to a subdomain.

43. (new) A processor-readable storage medium storing an instruction that, when executed by a processor, causes the processor to perform a method to reduce processing requirements on a client requesting secure content from a remote server over the Internet, the method comprising:

identifying a link to a secure webpage received from the remote server by the client;

rewriting the link to be recognizable by an intermediating device disposed between the client and the remote server;

enabling the intermediating device to intercept the rewritten link and retrieve the secure webpage;

receiving the requested secure webpage from the server onto the intermediating device; and

sending the requested secure webpage from the intermediating device to a client proxy.

44. (new) The processor-readable storage medium of claim 43 wherein the step of identifying a link to the secure webpage is selected to be performed by the client proxy.

45. (new) The processor-readable storage medium of claim 43 wherein the step of rewriting the link changes a secure request to a non-secure request.

46. (new) The processor-readable storage medium of claim 43 wherein the step of rewriting the link redirects a secure request to a subdomain.

47. (new) A system for accelerating delivery of secure socket layer webpages comprising,

a client web page browser installed in a computer operating in a network environment,

an intermediating server in the network environment addressable by the client web page browser,

a secure webpage server in the network environment addressable by the client web page browser in a manner requesting a secure connection,

a client proxy associated with the web page browser having software means for rewriting a first format address link to the secure webpage server requesting a secure webpage to a second format addressed to the intermediating server, the intermediating server having software means for rewriting the second format back to the first format for requesting and obtaining said secure web page from the secure webpage server via a secure connection, the intermediating server having software means for redelivery of said secure webpage to the client proxy and the client web page browser, whereby obtaining of secure webpages by the client web page browser from the secure webpage server is initially between the intermediating server and the secure webpage server and then between the intermediating server and the client web page browser.